Stephen R. Sady
Chief Deputy Federal Public Defender
steve_sady@fd.org
Steven T. Wax
Federal Public Defender
steve_wax@fd.org
Lisa Hay
Assistant Federal Public Defender
lisa_hay@fd.org
101 S.W. Main Street, Suite 1700
Portland, Oregon 97204
503-326-2123 Telephone
503-326-5524 Facsimile

Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA,	**Case No. 3:10-cr-00475-KI**
Plaintiff,	**MEMORANDUM IN SUPPORT OF ALTERNATIVE MOTION FOR SUPPRESSION OF EVIDENCE AND A NEW TRIAL BASED ON THE GOVERNMENT'S INTRODUCTION OF EVIDENCE AT TRIAL AND OTHER USES OF INFORMATION DERIVED FROM UNLAWFUL ELECTRONIC SURVEILLANCE**
v.	
MOHAMED OSMAN MOHAMUD,	
Defendant.	

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

FEDERAL CASES

DOCKETED CASES

FEDERAL STATUTES

MISCELLANEOUS

Introduction

The government belatedly provided notice that it introduced at trial and otherwise used information that was derived from electronic surveillance under 50 U.S.C. § 1881a, which is commonly known as § 702 of the Foreign Intelligence Surveillance Act (FISA). Section 702, which was enacted in 2008 as part of the FISA Amendments Act (FAA), constituted an unprecedented degradation of the privacy rights of Americans, with none of the protections that the First and Fourth Amendments require to limit governmental intrusions on privacy. The statute is unconstitutional under the First and Fourth Amendments because § 702:

- fails to provide judicial review of specific instances of searches and seizures of Americans' personal communications;
- fails to require probable cause, or any level of suspicion, before the government can search, seize, retain, and later access those communications;
- fails to require specificity regarding the individual targeted by – or the facility to be accessed during – the electronic surveillance;
- limits the FISA court's authority to insist upon, and eliminates its authority to supervise, instance-specific privacy-intrusion minimization procedures;
- provides no accountability regarding surveillance of individual Americans' electronic communications.

Under the statute's exclusionary remedy for the products of surveillance "not lawfully authorized or conducted" (50 U.S.C. § 1806(g)), and the constitutionally-based requirement of suppression of the fruit of the poisonous tree (*Murray v. United States*, 487 U.S. 533, 536-37 (1988)), the unlawfully derived material from warrantless surveillance in this case must be suppressed, including subsequent warrants, tactical decisions, and other resulting tangible and intangible things.

This is a highly unusual suppression motion because the government has provided no discovery regarding the circumstances under which the electronic surveillance was conducted, what information was obtained, and how it was used, and the Court has denied the defense motions for discovery. Basically, this motion seeks suppression of unknown evidence and other uses of information gathered at unknown times by unknown means by unknown persons and agencies operating under unknown protocols. At the end of this memorandum, the defense provides a number of questions for the Court to aid in its review that, by their detail and complexity, underscore the reasons for the continuing defense request that the Court find that full defense participation is "necessary" within the meaning of FISA or that the statutory limitation on defense participation is itself unconstitutional.

The factual background of this pleading can only be based on assumptions from the public record, including a heavily redacted 2011 opinion by the Foreign Intelligence Surveillance Court (FISC) and testimony before the Privacy and Civil Liberties Oversight Board (PCLOB) at a public hearing held on March 19, 2014.[1] The PCLOB information is of limited value for a number of

[1] The PCLOB is a an independent, bipartisan agency within the executive branch whose members are appointed by the President and confirmed by the Senate. PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 2 (Jan. 23, 2014). On March 19, 2014, the PCLOB held a hearing in which the General Counsels of the Federal Bureau of Investigation, the National Security Agency, and the Director of National Intelligence, as well as the Deputy Assistant Attorney General for the Department of Justice's National Security Division, provided testimony about programs operated under § 702. *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act Before The PCLOB* (2014) (transcript available at http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf) (PCLOB Hearing).

reasons: the witnesses did not purport to provide information regarding the protocols and practices in effect at the time of the surveillance in this case, which was probably between 2008 and 2010; the information provided was limited to declassified material; and the testimony was not under oath, not from individuals with first hand knowledge, and not subject to more than very limited questioning.

This Court writes on a clean slate about § 702 warrantless searches and seizures. Because the government has succeeded in challenging the standing of persons potentially affected by the warrantless surveillance programs, *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), this Court and a district court in Colorado are addressing constitutional and statutory challenges to the § 702 warrantless surveillance program for the first time. The FISC has apparently declined to view the statute's overall constitutionality as within its "narrowly circumscribed" job description. *In re Proceedings Required By § 702(i) Of The FISA Amendments Act Of 2008*, Misc. No. 08-01, 2008 WL 9487946, at *5 (FISC Aug. 27, 2008) (rejecting an offer of amicus to engage in constitutional analysis because "a generalized constitutional review, however, is not contemplated under Section 702(i)."). Further, no judicial ruling has come from the FISC in the context of "Cases" or "Controversies" within the constitutional meaning of Article III because only one party was involved. *Camreta v. Greene*, 131 S. Ct. 2020, 2028 (2011) (authority to adjudicate legal disputes requires adverse litigants with the "concrete adverseness which sharpens the presentation of issues") (quoting *Los Angeles v. Lyons*, 461 U.S. 95, 101 (1983)). No precedent results where decisions are made without the necessary concrete issues and adverse parties. *See Texas v. Cobb*, 532 U.S. 162, 169 (2001) ("Constitutional rights are not defined by inferences from opinions which did not address the question at issue."); *see also United States v. Booker*, 543 U.S. 220, 239-42 (2005) (limiting the

stare decisis effect of cases where the relevant constitutional issue was not raised by the parties or resolved by the court).

Although much of this brief addresses § 702 of the FAA, Section D argues that public disclosures regarding other surveillance programs should also result in disclosure and potential suppression or new trial based on the mass collection of telephone and internet metadata under separate statutory (and non-statutory) programs. Further, Section E argues that the government's post-trial notice also raises suppression issues the Court should address under the requirements of *Franks v. Delaware*, 438 U.S. 154 (1978), that applications for the later FISA warrants in this case should be subjected to a hearing regarding intentional or reckless false statements or material omissions regarding controverted facts.

I. Background Facts Regarding The § 702 Warrantless Electronic Surveillance Program

Congress enacted FISA in 1978 in response to outcries over unlawful warrantless intrusions on the privacy of American citizens conducted in the name of national security. 1 David S. Kris & J. Douglas Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, § 2:7 (2d ed. 2012). The Church Report found that the government, in the name of national security, had "violated specific statutory prohibitions," "infringed the constitutional rights of American citizens," and "intentionally disregarded" legal limitations on surveillance, including pursuing "a 'vacuum cleaner' approach to intelligence collection" that sometimes intercepted Americans' communications content under the pretext of targeting foreigners. *Final Report of the S. Select Comm. to Study Governmental*

Operations with Respect to Intelligence Activities, Book II, S. Rep. No. 94-755, at 137, 165 (1976).[2] While safeguarding against attacks by our Country's enemies was a central concern, the purpose of FISA was to rein in extra-legal activities by bringing governmental surveillance within the rule of law.

In 2008, the FAA increased radically the government's ability to search and seize the private electronic communications of American citizens and others protected by the Fourth Amendment. Individuals outside the United States, and who are not Americans (or "United States persons" under the statutory language), generally are not protected by the Fourth Amendment. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990). Section 702 allows the executive branch to target any "person" – which includes "any group, entity, association, corporation, or foreign power" (50 U.S.C. § 1801(m)) – that it reasonably believes is a non-U.S. person and located overseas, as long as a "significant" purpose of that interception is related to foreign intelligence.[3] Thus, the statute authorizes wholesale surveillance.

Based on public sources, the § 702 electronic surveillance program results in massive acquisition of individual Americans' telephone calls and emails with no individualized judicial supervision over the government's later reading of Americans' letters and listening to their telephone calls. A recently declassified FISC opinion from 2011 estimated that, in a single year, the programs implementing § 702 acquired more than 250 million communications. *[Case Name Redacted]*,

---

[2] *Accord* President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, 57-63 (Dec. 12, 2013).

[3] Foreign intelligence information is defined broadly under FISA. 50 U.S.C. § 1801(e).

[docket number redacted], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011). Reportedly, the National Security Agency (NSA) makes a copy of "nearly all cross-border text-based data," scans the content of each message using its chosen keywords or "selectors," then saves any communication that contains a match for further analysis. Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013.

By ostensibly targeting foreign "persons," the government "incidentally" searches and seizes the private communications of American citizens in contact with those foreign persons without complying with basic Fourth Amendment protections. The term "incidental" does not mean that these American communications are accidentally or unexpectedly collected or of lesser value than foreign communications. Where the government does accidentally or wrongly intercept communications – which, as described below, is inherent in at least one of the § 702 programs – it refers to these searches and seizures as "inadvertent." PCLOB Hearing at 12, 96-101. Although the government describes the collection of American communications as "inadvertent" and "incidental," the intrusions on Americans would more accurately be described as "inevitable" and "innumerable." Given the inherent breadth of collections under the § 702 programs, and the resulting capture of conversations of millions of Americans, the government's terminology trivializes the magnitude of the government's unsupervised acquisition of and access to Americans' private communications.

The following chart demonstrates how different § 702 is from other electronic surveillance statutes – traditional FISA and Title III wiretaps – in terms of what information must be presented to a neutral and detached judicial officer prior to engaging in individual searches and seizures:

	Title III	Traditional FISA	§ 702
Required level of suspicion of an individual	Probable cause the individual is committing, has committed, or is about to commit a criminal offense. 18 U.S.C. § 2518(3)(a).	Probable cause the individual is a foreign power (including terrorist organizations) or an agent of a foreign power. 50 U.S.C. § 1805(a)(2)(A).	None
Required level of suspicion regarding facility to be monitored	Probable cause communications concerning an offense will be obtained through interception. 18 U.S.C. § 2518(3)(b).	Probable cause each targeted facility is being used, or is about to be used, by a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(2)(B).	None
Particularity regarding individual to be monitored	Specify the identity, if known, of the person committing the offense or whose communications are to be intercepted. 18 U.S.C. § 2518(1)(b).	Specify the identity, if known, or a description of the specific target of the surveillance. 50 U.S.C. § 1805(c)(1)(A).	None
Particularity regarding location to be monitored	Specify the nature and location of the communications facilities as to which, or the place where, interception will occur. 18 U.S.C. § 2518(1)(b).	Specify the nature and location of each of the facilities or places at which the surveillance will be directed. 50 U.S.C. § 1805(c)(1)(B).	None
Particularity regarding types of communications to be intercepted	Particular description of the type of communication sought to be intercepted. 18 U.S.C. § 2518(1)(b).	Designate the type of foreign intelligence information being sought and the type of communications or activities to be subjected to the surveillance. 50 U.S.C. § 1805(c)(1)(C).	None

Recent PCLOB testimony described collection under § 702 through programs called Prism and Upstream. The government witnesses asserted that neither is a bulk collection method because, unlike the bulk telephone metadata collection under § 215 of the Patriot Act, both § 702 programs are presently "selector-based," meaning there is "some sort of discriminant" that directs the targeting.[4] PCLOB Hearing at 10. Thus, the 250 million communications collected in a single year, because they are generated by a massive number of selectors, are not considered "bulk" in intelligence jargon, even though they are gathered in a dragnet fashion, stored for up to five years, and accessed by subsequent queries. They are "bulk" in common understanding.

The identified "selector" for both programs is generally an email address, telephone number, or "something similar," perhaps Facebook or Skype account names. *Id*. at 25. The process appears to be that the government in some way will come across a "selector" believed to relate to foreign intelligence; the government will then do a "foreignness" evaluation to assess whether the person using that selector is located outside the United States and is not a United States citizen, using targeting procedures that are programmatically approved by the FISC on a yearly basis. If the selector is approved under the targeting procedures, then the method of collection will depend on whether Prism or Upstream is used.

[4] From the President's January 17, 2014, policy directive, the distinction regarding "bulk collection" for the purposes of the FAA appears to be merely semantic: "References to signals intelligence collected in 'bulk' mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)." Presidential Policy Directive – Signals Intelligence Activities, n.5 (Jan. 17, 2014).

Prism involves collection directly from a service provider, whether internet, like Google or Yahoo, or a telephone company. The government supplies the service provider with a "selector," and gets all future communications going "to or from" that selector. *Id*. at 25-26. This would mean that, for emails, the government obtains all emails coming into or being sent from a particular account, in addition to any historical content that is saved in that account. For telephones, the collection process appears to be indistinguishable from the type of FISA wiretap the FISC apparently eventually authorized against the defendant.

Upstream differs from Prism in that it also collects "about" communications and involves intercepting communications directly from the "Internet backbone." *Id*. at 26. This appears to mean the NSA is tapping into cables or servers in a location through which large amounts of data flow. Upstream collection uses some type of filtering technology that searches for communications coming "to" or "from" a certain selector and also any communications that are "about" that selector. *Id*. Thus, Americans' overseas communications will be collected even if they are not to or from a foreign target, but also if they contain a particular "selector" somewhere in the contents of the communication.[5]

However, Upstream "about" seizures cannot be limited to just those communications that include a specific selector. *[Case Name Redacted]*, 2011 WL 10945618, at *10. Such communications travel the internet in "packets" that often include totally unrelated communications

[5] The Court should heavily scrutinize the technology involved in this collection, as it appears the government may be indiscriminately searching every single electronic communication that crosses the "internet backbone."

and ones that are wholly domestic between United States citizens. Because the technology cannot discriminate well enough, this "about" collection will invariably intercept United States communications that should not have been intercepted. This method thus constitutes indiscriminate, bulk collection. Prior to 2011, these irrelevant, domestic communications were apparently included in a government database with the rest of the § 702 collections and were made available for later queries and searches without judicial supervision.

What happens next with the interceptions is guided by minimization procedures related to retention, accessing, dissemination, and other uses. As far as counsel can determine, the protocols in effect at the relevant times are still classified.[6] These procedures appear to provide little substance in terms of privacy protections for American citizens. For example, although there are requirements to purge American communications under limited circumstances when an individual analyst has recognized such a communication, there apparently is no requirement that an analyst actually look at any of the intercepted material. Instead, seized Americans' communications are apparently co-mingled with all other § 702 intercepts and retained in massive databases constructed by the different agencies. Those databases are available for later access and querying with no judicial oversight. Nor does there appear to be any effort to distinguish Americans' communications from other "acquired" material. Indeed, the government has even taken the position that it can later query the database with any "selector" – including ones known to be that of an American citizen – without implicating the Fourth Amendment. PCLOB Hearing at 39, 48, 78-79. This is despite the fact that the government

[6] What is declassified is that the FISC found some of the government's 2011 proposed minimization standards unconstitutional. *[Case Name Redacted]*, 2011 WL 10945618, at *28.

would not have been permitted to use that American selector in the initial targeting process, and § 702 explicitly bars reverse-targeting (i.e., targeting a foreign person for the purpose of intercepting U.S. communications). 50 U.S.C. § 1881a(b)(2).

Within this broad framework, the defense at this point in the litigation does not have the specific facts regarding the government's conduct of the search and seizure activity. However, as Senator Wyden stated on April 1, 2014, the collection and searches of American communications under § 702 is broad, warrantless, and constitutionally suspect:

> It is now clear to the public that the list of ongoing intrusive surveillance practices by the NSA includes not only bulk collection of Americans' phone records, but also warrantless searches of the content of Americans' personal communications. This is unacceptable. It raises serious constitutional questions, and poses a real threat to the privacy rights of law-abiding Americans. If a government agency thinks that a particular American is engaged in terrorism or espionage, the Fourth Amendment requires that the government secure a warrant or emergency authorization before monitoring his or her communications. This fact should be beyond dispute.

Press Release, *Wyden, Udall On Revelations That Intelligence Agencies Have Exploited Foreign Intelligence Surveillance Act "Loophole*," Apr. 1, 2014. In this context, the Court will need to have a broad range of information regarding the techniques and protocols for each level of intrusion into Americans' communications: the acquisition of the internet letters and telephone calls; the sorting and organization of data; the conditions of retention; the accessing of the communications; and dissemination and other uses of the contents of the communications. This involves determinations of targeting and minimization protocols and procedures for each of the relevant agencies, and complicated technical questions regarding American-sourced communications, encryption and

decryption, scanning and searching, and involvement of individual analysts reading and listening to actual content.

Rather than speculating regarding the many ways the targeting and minimization procedures have failed to meet Fourth Amendment standards, and speculating how those procedures applied at different stages of the collection of American communications, the defense again suggests that the only fair way to litigate the case involves the full adversary process. This is especially true given the statement by Senator Wyden, who serves on the Senate Select Committee on Intelligence, that the agencies have in the past made misleading suggestions regarding this type of search and seizure activity:

> Senior officials have sometimes suggested that government agencies do not deliberately read Americans' emails, monitor their online activity or listen to their phone calls without a warrant. However, the facts show that those suggestions were misleading, and that intelligence agencies have indeed conducted warrantless searches for Americans' communications using the 'back-door search' loophole in section 702 of the Foreign Intelligence Surveillance Act. Today's admission by the Director of National Intelligence is further proof that meaningful surveillance reform must include closing the back-door searches loophole and requiring the intelligence community to show probable cause before deliberately searching through data collected under section 702 to find the communications of individual Americans.

Id.

Because § 702 does not provide sufficient Fourth Amendment protections to the private communications of American citizens, the statute is unconstitutional. If the statute could be construed to provide protections coextensive with the Fourth Amendment, then the government activity in this case failed to comply with those limits and violated the statute and Constitution. As Senator Wyden stated, "Because Section 702 does not involve obtaining individual warrants, it

contains language specifically intended to limit the government's ability to use these new authorities to deliberately spy on Americans." *Id*. Individualized judicial supervision is a necessary check before the government accesses the content of Americans' communications.

II. Legal Arguments Requiring Suppression Of Evidence And A New Trial Based On Constitutional, Statutory And Procedural Violations

A. The Warrantless Electronic Surveillance Statute That Resulted In Derivative Evidence And Uses Against The Defendant Violated The Fourth Amendment.

The warrantless mass collection, retention, accessing, dissemination, and use of the contents of Americans' electronic communications violate the Fourth Amendment of the Constitution, which states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

See United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 313 (1972) (*Keith*) (warrantless domestic surveillance for national security purposes violates the Fourth Amendment); *Berger v. New York*, 388 U.S. 41 (1967) (statute that authorized electronic surveillance under judicial supervision violated the Fourth Amendment because it "permits a trespassory invasion of the home or office, by general warrant, contrary to the command of the Fourth Amendment."). Although the defense recognizes that the Fourth Amendment may have no application to foreign persons outside the United States, the § 702 programs permit the widespread capture, retention, and later querying, dissemination, and use of the communications of American citizens, all without any of the protections required by the Fourth Amendment.

The Court's assessment of § 702's constitutionality should take into account other constitutional interests that are closely related to the Fourth Amendment. Where searches and seizures involve First Amendment protected materials – here, communications implicating association, religion, press, and speech rights – the Fourth Amendment must "be applied with 'scrupulous exactitude.'" *See Armstrong v. Asselin*, 734 F.3d 984, 993-94 (9th Cir. 2013) (quoting *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978)). The Supreme Court recognized the danger that warrantless surveillance would chill constitutionally protected speech:

> National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech . . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

Keith, 407 U.S. at 313-14.[7]

The intrusions in this case also implicate the separation of powers doctrine, which inheres in the structure of checks and balances created by the first three Articles of the Constitution:

> The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that *individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government*. The independent check upon executive discretion is not satisfied, as the Government argues, by 'extremely limited' post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances which

[7] The First Amendment – in addition to informing the Fourth Amendment analysis – provides an independent basis for finding § 702 unconstitutional because the mass government surveillance dramatically chills protected speech and association. *Infra* at Section II B.

> failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.

Keith, 407 U.S. at 317-18 (emphasis added) (footnotes and citations omitted). The intimate personal facts revealed by the government's perusal of one's electronic communications also infringe on the liberty protected by the Due Process Clause. *Compare Berger*, 388 U.S. at 63 ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."), *with Lawrence v. Texas*, 539 U.S. 558 (2003), ("Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.").

Under well-established Fourth Amendment law, § 702 fails to meet constitutional requirements for three reasons. First, under the Warrant Clause, the § 702 program of acquiring, retaining, and later accessing Americans' electronic communications is presumptively unreasonable because it fails to meet the constitutional requisites for valid Fourth Amendment warrants that are intended to interpose a neutral and detached magistrate between the citizen and the government. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971) ("[T]he most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well delineated exceptions.'") (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)); *accord Arizona v. Gant*, 556 U.S. 332, 338 (2009). Second, the warrantless searches and seizures do not pass constitutional muster because the government cannot establish one of the "jealously and carefully drawn" exceptions to the warrant requirement. *Georgia v. Randolph*, 547 U.S. 103, 109 (2006) (quoting *Jones v. United States*, 357 U.S. 493, 499 (1958)). Third, if the

interest were not within the core zones of privacy protected by the Warrant Clause, which is not the case with Americans' private communications, the searches and seizures would still be unreasonable given the balance of interests involved, especially given the radical departure from each of the requisites for compliance with the Warrant Clause's protection of individual rights. The three-step analysis applies to each phase of the § 702 activity related to Americans' communications, including but not limited to initial acquisition, retention, accessing by queries or otherwise, and dissemination or other use.

1. The Government's Program That Resulted In The Search And Seizure Of The Content Of An American Citizen's Electronic Communications Violated The Warrant Clause Of The Fourth Amendment In Six Ways, Any Of Which Renders The Warrantless Collection, Retention, And Dissemination Program Presumptively Unconstitutional.

The contents of American citizens' telephone calls and emails are within the core zone of privacy protection from government intrusion in the absence of a warrant. *United States v. Alderman*, 394 U.S. 165, 177 (1969); *United States v. Katz*, 389 U.S. 347, 353 (1967); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). "[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." *Keith*, 407 U.S. at 313. Electronic surveillance requires compliance with the "basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded." *Berger*, 388 U.S. at 63.

Just as letters and packages in the mail are treated as Fourth Amendment "papers" within the "home," the content of electronic communications are protected against having police officers read them in the absence of a warrant.

> Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizure extends to their papers, thus closed against inspection, wherever they may be. *Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household*. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.

Walter v. United States, 447 U.S. 649, 655 (1980) (emphasis added). The Fourth Amendment's protections apply to international as well as domestic communications. *See United States v. Ramsey*, 431 U.S. 606, 616-20 (1977); *United States v. Peterson*, 812 F.2d 486, 490-92 (9th Cir. 1987). The Fourth Amendment applies beyond criminal investigations because it "guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government," *Skinner v. Railway Labor Executives' Assn*., 489 U.S. 602, 613-14 (1989), "without regard to whether the government actor is investigating crime or performing another function," *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010), including protecting national security, *Keith*, 407 U.S. at 313-14.

The Warrant Clause presupposes a number of measures that are missing from the search and seizure of the defendant's electronic communications under the FAA: a) a warrant authorizing the

search and seizure; b) based upon probable cause; c) particularly describing the place to be searched and the items to be seized; d) based on an affidavit under oath or affirmation; e) issued by a neutral and detached magistrate operating in a judicial capacity; f) with a return or other procedure assuring compliance with the terms of the warrant in its execution. The absence of these features from FAA surveillance is relevant to two aspects of Fourth Amendment analysis. First, because these features are absent from the program resulting in the search and seizure of the private communications of persons who reasonably should be known to be Americans, and the absence of any single factor would violate the Warrant Clause, the Court should hold that the government's warrantless collection, retention, and accessing are presumptively unreasonable under *Coolidge* and *Gant*. Second, to the extent reasonableness is at issue, the extreme disconnect between § 702 procedures and the basic Fourth Amendment warrant protections demonstrates the unreasonableness of the searches and seizures.

a) The Warrant Clause Requires A Fourth Amendment "Warrant," Whereas § 702 Permits Search And Seizure With Only A General "Authorization" For Programmatic Surveillance.

The "warrant" of the Warrant Clause is distinct from the programmatic "authorization" and "certificate" by the FISC under 50 U.S.C. § 1881a(a) and (g). The issuance of a search warrant by a judge involves individualized determination regarding the constitutionality of a specific invasion of privacy:

> In response to these abuses of power by the government, *the Founders* abolished general warrants, restricted the government's ability to search without warrants, and *required individual authorization of specific warrants*. *Today, search warrants are specific instruments that restrict government, dictate who may conduct a search,*

> *what may be searched, and when it may be searched*. Both the procurement of the search warrant and its execution must be done under the law; otherwise the search is an unconstitutional abuse of governmental power.

Swate v. Taylor, 12 F. Supp. 2d 591, 594 (S.D. Tex. 1998); *see also In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 854 (9th Cir. 1991) ("Subpoenas are not search warrants."). In contrast, § 702 only calls for an "authorization" that does not involve any of the specificity of a Fourth Amendment warrant. As former FISC Judge Robertson pointed out, the programmatic authorizations and certificates involved with FAA surveillance do not involve the type of judicial review that is normally provided for the issuance of search warrants. Transcript of PCLOB Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act at 36 (July 9, 2013)[8] ("[T]hat's not the bailiwick of judges.").

The Fourth Amendment's protections require a warrant, not a generalized permission to conduct massive collection of Americans' communications and to access them without an individualized determination that an American citizen's electronic communications can be seized and read, secretly and without consent, by government agents. *See Dalia v. United States*, 441 U.S. 238, 256 n.18 (1979) ("electronic surveillance undeniably is a Fourth Amendment intrusion requiring a warrant); *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985) ("even narrowly circumscribed electronic surveillance must have prior judicial sanction.").

[8] Available at http://www.pclob.gov/All%20Documents/July%209,%202013%20Workshop%20Transcript.pdf

b) The Warrant Clause Requires That The Search And Seizure Be Based On Probable Cause, Whereas § 702 Permits Seizure Without Individualized Suspicion.

The Fourth Amendment's requirement of "probable cause" assures that "baseless searches shall not proceed." *Keith*, 407 U.S. at 316. This fundamental norm for government searches and seizures requires sworn facts sufficient for a judge to decide whether individualized suspicion justifies the government's intrusion on privacy. *See Gates v. Illinois*, 462 U.S. 213, 239 (1983) ("An affidavit must provide the magistrate with a substantial basis for determining the existence of probable cause, which is not met by wholly conclusory statements"). The Supreme Court has carefully guarded the probable cause standard against encroachment within core areas of privacy. As held in *Arizona v. Hicks*, even a minor intrusion beyond the boundary of the lawful government action, where core rights are concerned, requires probable cause. 480 U.S. 321, 329 (1987).

On its face, § 702 does not require the government to have individualized suspicion or probable cause before engaging in electronic surveillance. The statute allows the government to target any "persons reasonably believed to be located outside the United States to acquire foreign intelligence information," (50 U.S.C. § 1881a(a)), with the definition of "person" broadly defined to include "any group, entity, association, corporation, or foreign power," (50 U.S.C. § 1801(m)). While the FISC approves general programs and procedures under § 702, it does not review or approve the government's specific targeting decisions or its later access and querying of any seized communications. Given the broad definition of "person" and the minimal requirement that the electronic surveillance have as "a significant purpose" the acquisition of foreign intelligence (50 U.S.C. § 1881a(a)(2)(v)), the statute broadly authorizes the government to target entire geographical

areas or groups of people. Thus, without court approval, § 702 could authorize the government to intercept and read every American communication with a country of interest – Iran or Yemen, for example – as long as the government satisfies *itself* that such intercepts implicate foreign intelligence.

The probable cause standard has been the fundamental bulwark protecting Americans from governmental over-reaching into their private lives over the centuries leading up to and following the ratification of the Bill of Rights. *United States v. Winsor*, 846 F.2d 1569, 1576-77 (9th Cir. 1988) (en banc); *see Kyllo v. United States*, 533 U.S. 27, 34 (2001) (requiring a warrant for use of a thermal imaging device outside the home because "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.").[9] The government's reading of the contents of American citizens' electronic communications should only be permissible based on a judicial finding of probable cause. Under § 702, because no probable cause or other level of suspicion is required before communications are acquired, retained, and read, the statute does not comply with the Warrant Clause.

[9] While the Supreme Court has suggested the possibility that area warrants based on a judicial finding of reasonable suspicion could be reasonable, those cases have involved only areas of low privacy and minor intrusions. *See Davis v. Mississippi*, 394 U.S. 721, 727-28 (1969) (detention for fingerprinting "might, under narrowly defined circumstances," comply with the Fourth Amendment) (citing *Camara v. Municipal Court*, 387 U.S. 523 (1967) (housing inspections reasonable "[i]f a valid public interest justifies the intrusion contemplated, then there is probable cause to issue a suitably restricted search warrant").

c) The Warrant Clause Requires Particularity Regarding The Places To Be Searched And The Items To Be Seized, Whereas § 702 Permits Generalized And Programmatic Acquisition, Retention, And Accessing Of Electronic Communications.

One of the primary motivations behind the Fourth Amendment's particularity requirement was to protect against general searches. *Marron v. United States*, 275 U.S. 192, 196 (1927). Wholesale seizure of documents is exactly "the kind of investigatory dragnet that the Fourth Amendment was designed to prevent." *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982). The purpose of the specificity requirement is to prevent general exploratory rummaging in a person's belongings. *Coolidge*, 403 U.S. at 467. "As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron*, 275 U.S. at 196.

The particularity requirement has two aspects: for the warrant to be valid, the items to be seized must be stated with particularity, *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986), and the location to be searched must be specified, *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The programmatic surveillance under § 702 involves no particularity requirement as to specific items or specific locations or facilities, either before the acquisition or prior to accessing seized electronic communications. As with the electronic surveillance statute involved in *Berger*, § 702 has no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor 'the place to be searched,' or 'the persons or things to be seized' as specifically required by the Fourth Amendment. 388 U.S. at 56. In fact, § 702 specifically removed the previous requirement of particularity as to the facility targeted. 50 U.S.C. § 1881a(g)(4) (certification not required to identify the specific "facilities, places, premises or property" at which the acquisition is directed or

conducted). Section 702 provides inadequate specificity regarding the American communications to be retained and assessed to guard against the grave dangers against which a search warrant for electronic information protects. *See Sedaghaty*, 728 F.3d at 914 (search warrant limited scope of computer search). Under § 702, the communications of American citizens are swept up in the dragnet fashion that led to the promulgation of the Warrant Clause.

d) The Warrant Clause Requires A Statement Under "Oath Or Affirmation," Whereas § 702 Has No Such Requirement.

The Warrant Clause explicitly requires that probable cause be supported by a statement under "Oath or affirmation." This phrase "is a formal assertion of, or attestation to, the truth of what has been, or is to be, said." *United States v. Bueno-Vargas*, 383 F.3d 1104, 1110 (9th Cir. 2004) (quoting *United States v. Brooks*, 285 F.3d 1102, 1105 (8th Cir. 2002)). "The oath or affirmation subjects the person making it to the penalties for perjury." *Id*. The sworn information must be contained within the four corners of the affidavit because a contrary rule, allowing for later supplementation with extrinsic facts, would "render the warrant requirements of the Fourth Amendment meaningless." *Whitely v. Warden*, 401 U.S. 560, 564 n.8 (1971). The true test for compliance with this aspect of the Warrant Clause is whether perjury could be charged for any material allegation that was false. *Bueno-Vargas*, 383 F.3d at 1111. The statements under penalty of perjury must relate to the truth of the information supporting the suspicion. *Levine v. City of Bothell*, 904 F.Supp2d 1124, 1130 (W.D.Wash. 2012).

In contrast, § 702 surveillance appears to be based on a "determination" by the Attorney General and the Director of National Intelligence. 50 U.S.C. § 1881a(c)(2). The provision for a

supporting affidavit does not purport to involve probable cause and appears to be optional: the Attorney General and the Director of National Intelligence, prior to authorization, shall provide the FISC "a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection." 50 U.S.C. § 1181a(g)(1)(A). The certification does not deal with particular persons or events, but only to the procedures to be followed. 50 U.S.C. § 1181a(g)(2). The § 702 procedures fall far short of the "Oath or affirmation" provision of the Fourth Amendment's Warrant Clause.

e) The Warrant Clause Requires Review By A Neutral and Detached Magistrate, Whereas § 702 Blurs The Judicial Role By The FISC's Participation In The Construction Of The Executive Branch's Program.

The text of the Fourth Amendment requires the interposition of a neutral and detached magistrate between the individual citizen and the police office engaged in "the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 14 (1948); *see McDonald v. United States*, 335 U.S. 451, 455-56 (1948) (discussing the need for "an objective mind [to] weigh the need to invade" privacy to enforce the law). Where the role of the judge is reduced to consulting with the Executive Branch, with no case or controversy involving an adversary, the judge's input regarding the program no longer qualifies as judging, but only provides a non-judicial advisory opinion. *See Chafin v. Chafin*, 133 S. Ct. 1017, 1023 (2013) (federal courts may not "give 'opinion[s] advising what the law would be upon a hypothetical state of facts.") (quoting *Lewis v. Continental Bank Corp.*, 449 U.S. 472, 477 (1990)). As in cases where the judicial and executive functions are blurred, the absence of the constitutionally required judicial interposition between a

citizen and the government, resolving the specific competing interests of specific parties, results in failure to meet the fundamental separation of powers function of the Warrant Clause. *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979) (where magistrate participated in search, "the objective facts of record manifest an erosion of whatever neutral and detached posture existed at the outset"); *Coolidge*, 403 U.S. at 449.

Given the programmatic "approval" process performed by the FISC under § 702, the court no longer functions as neutral and detached judicial officers. The statutory function is not to issue a warrant based on probable cause but to authorize and certify a program. 50 U.S.C. § 1881a(a). In doing so, the FISC meets ex parte with the government and assists in formulating the program. *See [Case Name Redacted]*, 2011 WL 10945618, at *1-3. Rather than approve or disapprove of proposals, the FISC has a role in designing them. The program reviews are more like administrative than judicial action. Whether a magistrate is neutral and detached in a particular case is "an individualized and contextual inquiry[, and] [c]ourts must focus on the specific circumstances surrounding the issuance of the warrant and decide whether the magistrate 'manifested that neutrality and detachment demanded of a judicial officer when presented with a warrant application for a search and seizure.'" *Coolidge*, 403 U.S. at 453 (quoting *Lo-Ji Sales*, 442 U.S. at 326).

Given the blurred lines in the present case, the FISC did not operate as the neutral and detached magistrate required by the Warrant Clause. FISC proceedings do not involve constitutional "Cases" and "Controversies," instead providing, in effect, advisory opinions. *See Camreta*, 131 S. Ct. at 2028. To the extent the FISC participates in creation of surveillance programs, rather than judging the adequacy of applications for searches, the court's legislative actions may also violate the

non-delegation doctrine. *Mistretta v. United States*, 488 U.S. 361, 371-72 (1989) (the non-delegation doctrine states that "'the integrity and maintenance of the system of government ordained by the Constitution' mandate that Congress generally cannot delegate its legislative power to another Branch.") (quoting *Field v. Clark*, 143 U.S. 649,692 (1892)). Unlike the usual delegation issues, judicial participation in formulating surveillance programs does not involve legislative rule-making by agencies, with opportunities for public notice and comment, but direct judicial action, in secret, with the executive branch.

f) The Warrant Requirement Assumes Some Form Of Accountability Through Notice And A Return To An Issuing Judge, Whereas § 702 Includes No Form Of Notice Or Accountability.

Federal search warrants assure particularity by requiring specificity in the contents of the warrant and a return upon its execution. Fed. R. Crim. P. 41(e) and (f). The "high function" of the Fourth Amendment's warrant's requirement "is not necessarily vindicated when some other document, somewhere, says something about the objects of the search, but the contents of that document are neither known to the person whose home is being searched nor available for her inspection." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). In *Groh*, the Court held that officers leading a search team must "mak[e] sure that they have a proper warrant that in fact authorizes the search and seizure they are about to conduct . . . . That is not a duty to proofread; it is, rather, a duty to ensure that the warrant conforms to constitutional requirements." 540 U.S. at 563 n.6 (quoting *Ramirez v. Butte-Silver Bow County*, 298 F.3d 1022, 1027 (9th Cir. 2002)); *see also United States v. Gantt*, 194 F.3d 987, 991 (9th Cir. 1999), *overruled on other grounds*, *United States v. W.R.*

Grace, 526 F.3d 499 (9th Cir. 2008). The notice and return aspects of Fourth Amendment warrants assure particularity by assuring "the individual whose property is searched and seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." *Groh*, 540 U.S. at 563-64; *see United States v. Metter*, 860 F.Supp.2d 205, 215 (E.D.N.Y. 2012) (Fourth Amendment requires execution of computer search within a reasonable time).

The return, or notice of seizure, should also be required by due process because notice of a search is necessary to any available remedies regarding the execution of the search and seizure. *City of West Covina v. Perkins*, 525 U.S. 234, 240 (1999) ("when law enforcement officers seize property pursuant to warrant, due process requires them to take reasonable steps to give notice that the property has been taken so the owner can pursue available remedies for its return."). In striking down the wiretap statute in *Berger*, the Court pointed out that, like the FAA, the New York statute "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts." 388 U.S. at 60. The Ninth Circuit has held that, in the context of the intangibles at issue with surreptitious entries, the absence of a notice requirement casts strong doubts upon a warrant's constitutional adequacy "because surreptitious searches and seizures strike at the heart of the interests protected by the Fourth Amendment." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986).

> The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed. The warrants in this case failed to do so.

Id. The same reasoning and passion are implicated here because the FAA programmatic surveillance lacks any procedure remotely resembling notice and accountability when the government intercepts Americans' private communications. The American citizen is never notified that private communications were seized and read; the searchers receive no guidance regarding the limits of what can be read; and there is no return or other process by which the FISC can know whether the communications of American citizens were within or beyond the scope of the authorization.

2. The Intelligence Agencies' Claim That, Once Communications Are Acquired, The Fourth Amendment No Longer Applies Runs Contrary To Supreme Court And Ninth Circuit Precedent.

Whatever arguments the government could make for wholesale acquisition of Americans' communications – which the defense believes itself fails to meet constitutional requirements – they do not apply to retention, querying, dissemination, and other use of Americans' communications without a warrant. Before the PCLOB, the intelligence agencies asserted that, once communications are acquired, "subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody." PCLOB Hearing at 28. On the contrary, Supreme Court precedents reject that premise. Even where an officer is lawfully in a home, the Court rejected a standard lower than probable cause for a further intrusion, even a minor one, where an officer picked up a record player to read its identification number, holding that "the textual and traditional standards of probable cause" had already set the proper standard for the additional search. *Hicks*, 480 U.S. at 329. For all but "narrowly defined intrusions, the requisite 'balancing' has been performed in centuries of precedent and embodied in the principle that 'seizures' are 'reasonable'

only if supported by probable cause." *Winsor*, 846 F.2d at 1576-77 (quoting *Dunaway v. New York*, 442 U.S. 200, 213-14 (1979)).

The PCLOB testimony that "I don't think there are any other contexts really in general in which a warrant is required to search information already in your custody" simply reflects a profound misunderstanding of basic Fourth Amendment law. In this very case, although the Court ultimately did not reach the merits, the government seized the defendant's computer with a limited consent. While the computer was "already in the government's custody," in the language of the PCLOB witness, Supreme Court and other precedent require a warrant for any search beyond the scope of the consent. CR 57 at 7-9 (citing among others *Florida v. Jimeno*, 500 U.S. 248, 251 (1991), and *United States v. Runyan*, 275 F.3d 449, 463-64 (5th Cir. 2001)). Similarly, computer searches beyond the scope of terms authorized by the warrant are considered warrantless searches. *United States v. Sedaghaty*, 728 F.3d 885, 910-13 (9th Cir. 2013) (rejecting expansion of the scope of computer search authorized by warrant); *see also United States v. Mulder*, 808 F.2d 1346, 1348 (9th Cir. 1987) (pills lawfully in government possession required warrant for testing); *United States v. Young*, 573 F.3d 711, 720-21 (9th Cir. 2009) (closed containers in government possession required warrant to search contents); *United States v. Crist*, 627 F.Supp.2d 575, 585 (M.D. Pa. 2012) (search of hard drive using EnCase required warrant to the extent the search exceeded the scope of private search).

Separate analyses under the Fourth Amendment are required not only at each stage of the process – acquisition, retention, query, dissemination, use, and so forth – but also based on the different protocols, practices, and activities of the different agencies. The agencies each have

separate protocols and databases. PCLOB Hearing at 18-19. Each step and each agencies' practices implicate American citizens' Fourth Amendment rights.

3. The § 702 Programmatic Electronic Surveillance Of The Writings Of American Citizens Does Not Fall Within A Well-Established, "Jealously And Carefully" Drawn Exception To The Warrant Requirement.

The Supreme Court has never held that there is a foreign national security exception to the Warrant Clause, but to the extent one exists, its scope is far narrower than the massive surveillance program involving acquisition, retention, and accessing of the emails and telephone calls of millions of American citizens. The Supreme Court in *Keith* held that there is no exception to the Fourth Amendment's warrant requirement for domestic national security surveillance. 407 U.S. at 320.[10] The reasoning regarding domestic national security very closely parallels the reasons that any exception to the warrant requirement for foreign national security concerns should not encompass mass collection, retention, accessing, and later use of American electronic communications and telephone calls.

The policies and reasoning undergirding the Supreme Court's decision in *Keith* finding no domestic national security exception to the Warrant Requirement should govern this case. *Keith* involved the warrantless wiretapping for the national security purposes of investigating the bombing

[10] As noted above, however, the Upstream method of collection under § 702 does, in fact, search and seize entirely domestic communications. Moreover, the government cannot even claim a national security exception as to many of these communications because the government has no idea beforehand what exactly it is seizing and searching. To the extent government technology reviews every piece of data traversing the "Internet backbone," the government is constantly searching domestic communications indiscriminately in hopes of finding foreign intelligence information.

of a Central Intelligence Agency office. The government argued that national security provided an exception to the Supreme Court's requirement of a warrant for electronic surveillance as otherwise required by *Berger* and *Katz*. After noting that the case only involved domestic national security because no foreign power was involved, the Court addressed the question left open in *Katz*: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security." *Keith*, 407 U.S. at 309 (quoting *Katz*, 389 U.S. at 358 n.23). In the domestic context, the answer was a firm "no."

After recognizing the real threats to national security, the Court found that the dangers of intrusions on privacy through electronic surveillance required judicial supervision:

> But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development – even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance . . . . Our decision in Katz refused to lock the Fourth Amendment into instances of actual physical trespass. Rather, the Amendment governs 'not only the seizure of tangible items, but extends as well to the recording of oral statements . . . without any 'technical trespass under . . . local property law.' . . . . That decision implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.

Keith, 407 U.S. at 312-13 (footnotes and citations omitted).

In holding that the Warrant Clause applied to domestic national security cases, the Court also took into account the First Amendment interests affected by warrantless electronic surveillance. *Id*. at 313-14 ("National security cases, moreover, often reflect a convergence of First and Fourth

Amendment values not present in cases of 'ordinary' crime."). Given the centrality of the privacy interests at stake, the Court rejected the government's claim of authority unlimited by the Warrant Clause to spy on Americans' electronic communications:

> These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute . . . . But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

Id. at 316-17. As a consequence, even if in hindsight the surveillance was arguably reasonable, the government's access to electronic communications violated the Fourth Amendment's requirement of a prior authorization for such an intrusion by a neutral and detached magistrate. *Id*. at 317-18. In rejecting the government's request that domestic national security should form one of the exceptions to the warrant requirement, which the Court described as "few in number and carefully delineated," *id*. at 318, the Court listed out the dangers of unreviewed and unreviewable electronic surveillance:

> Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a

> manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

Id. at 320.

To the extent any national security exception exists, the "jealously and carefully" drawn parameters, *Randolph*, 547 U.S. at 109, should be no broader than the FISA's authorization for "electronic surveillance without a court order," which explicitly protects the private communications of Americans by requiring that:

> (A) the electronic surveillance is solely directed at—
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801 (a)(1), (2), or (3) of this title; or
>
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title;
>
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; . . .

50 U.S.C. § 1802. Any construction of an exception beyond this narrow definition would undermine the FISA's purpose of curbing "the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(1); *see also In re National Security Telecommunications Records Litigation*, 564 F. Supp. 2d 1109, 1117 (N.D. Cal. 2008) (FISA's repeal of 18 U.S.C. § 2511(3) eliminated "any congressional recognition or suggestion of inherent Presidential power with respect to [foreign intelligence] electronic surveillance.") (quoting S. Rep. 95-701, 72).

Whatever the outer limits of a national security exception, the mass collection and accessing of American electronic communications under § 702 programs in effect during the relevant years far exceeded any "carefully delineated" boundary, thereby implicating the same First and Fourth Amendment interests protected under the *Keith* opinion. Just as in *Keith*, the dangers to Americans' privacy far outweigh the circumvention of the judiciary in making individualized determinations regarding the invasion of core areas of privacy:

> Thus, we conclude that the Government's concerns do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance. Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values. Nor do we think the Government's domestic surveillance powers will be impaired to any significant degree. A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review. By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur.

Id. at 321. Under the FAA warrantless surveillance program, Americans suffer the type of "indiscriminate wiretapping and bugging of law-abiding citizens" – magnified by advancing technology – that the Fourth Amendment was designed to prevent. No clearly-established and well-defined exception to the Warrant Clause allows the general searches of Americans' communications that occurred under the FAA surveillance program.

As with analysis of the warrant requirement, analysis of the existence of any exception to the warrant requirement must include not only the initial acquisition but also the retention, query, dissemination, use, and other such activity. And, again, because different intelligence agencies have different policies, practices, and databases, the Court must analyze the search and seizure activities

separately based on each agencies' actions. In sum, no constitutionally permissible exception justifies warrantless and unlimited searches, queries, or use of the communications of American persons whose communications were obtained because the government proceeded against a foreign national outside the ambit of the Fourth Amendment.

4. The Electronic Surveillance In This Case Was Unreasonable Within The Meaning Of The Fourth Amendment.

In areas outside of core zones of privacy, government searches and seizures can be deemed reasonable based on a balancing of the intrusion against the government's need. *Terry v. Ohio*, 372 U.S. 1, 21-23 (1968) (stop and frisk on a public street based on reasonable suspicion based on articulable facts); *Camara v. Municipal Court*, 387 U.S. 523, 534-535 (1967) (administrative searches for housing safety violations). The court only weighs reasonableness of intrusions based on less than probable cause when the searches "occur in certain clearly defined places which by their public nature give rise to reduced expectations of privacy." *Winsor*, 846 F.3d at 1576. Because Americans' private communications are within the core zone of privacy, such a reasonableness analysis is inappropriate.

The Supreme Court in *Keith* noted the type of balancing that might pass constitutional muster by analogy to administrative warrants in *Camera*:

> Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.
>
> It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of [the wiretap

> statute] but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court (e.g., the District Court for the District of Columbia or the Court of Appeals for the District of Columbia Circuit); and that the time and reporting requirements need not be so strict as those in [the wiretap statute].

Id. at 323. Congress responded by creating such a varied form of warrant application under FISA, with its many analogs to traditional Fourth Amendment requisites. As this Court ruled on the pretrial FISA motion, the individualized procedures required for FISA surveillance – which include individualized suspicion and direct judicial oversight – passed constitutional muster. Section 702, however, falls far short of even those lesser standards. *See* comparison chart, *supra*, at 7.

For the contents of Americans' communications, any balancing of interests has already been performed by the Constitution: a particularized warrant, based on probable cause, is necessary for the government to collect and read the content of, or listen to, Americans' private conversations. The § 702 programs are unprecedented in terms of the unlimited scope of the collections and the lack of any particularized suspicion to support this massive acquisition of Americans' communications.

The minimization provisions of 50 USC § 1881a do not provide adequate protection to Americans because they do not provide adequate standards and supervision for gathering, retention, query, dissemination, and use of Americans' communications. Congress recognized in enacting § 1881a that it could only allow warrantless surveillance of the type permitted under § 702 on foreign nationals outside the United States. As a result, the statute includes the requirement that any activity undertaken under its provisions must be consistent with the Fourth Amendment. 50 USC 1881a (b)(5). The statute then seeks to provide protection to Americans through minimization procedures

set out in subsection (e). That subsection, however, has no substantive content. Rather, it refers to 50 USC §§ 1801(h) and 1821(4). Review of those subsections reveals that they provide no meaningful protection. As a result, the statute on its face fails to provide the protection required under the Fourth Amendment, and any search and seizure activity taken under it violates Americans' rights.

The deficiencies in subsection (h) are readily apparent. At the outset, subsection (h)(1) requires the adoption of minimization procedures that are "designed in light of the purpose and technique of the particular surveillance." That subsection then concludes with a prohibition on dissemination, only limiting dissemination to what is "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence." The exclusions from and limits on the minimization procedures swallow the rule. As long as the Attorney General believes that information about a United States person has some bearing on foreign intelligence, he can do whatever he wants with it. Because the minimization procedures are weak, ineffective, and illusory, the statute is unconstitutional as unreasonable and impermissibly general as to Americans. Therefore, the fruits of any information obtained may not be used against a United States person.

B. The Warrantless § 702 Program Violates The First Amendment Because Its Breadth And Vagueness Chill Americans' Exercise Of First Amendment Rights.

If a statute operates to chill or suppress exercise of speech and association protected by the First Amendment by reason of vague terms or overbroad coverage, the statute is invalid. *Nevada Comm'n of Ethics v. Carrigan*, 131 S.Ct. 2343, 2353 (2011) (Kennedy, J., concurring) (citing *United States v. Williams*, 553 U.S. 285 (2008)); *see also Ashcroft v. Free Speech Coalition*, 535 U.S. 234,

244 (2002) ("The Constitution gives significant protection from overbroad laws that chill speech within the First Amendment's vast and privileged sphere."). The § 702 provisions related to acquisition, retention, accessing, and other use of Americans' communications include no discernible limits on the terms for intrusions or the breadth of coverage regarding Americans. As a consequence, the statute has deeply chilled Americans' use of the internet and telephones to express themselves and to form associations with others.

The specter of NSA warrantless surveillance has cast a real and pervasive chill over Americans' exercise of First Amendment rights. Ordinary Americans – present counsel included – hesitate and self-censor before communicating by electronic means previously considered private. People like the *Clapper* plaintiffs profoundly changed their business practices out of concern for government spying. 133 S. Ct. at 1156-57 (describing how the contrast between FISA and § 702 standards affected lawyers, journalists, and human rights researchers) (Breyer, J., dissenting).[11] Even former President Jimmy Carter abandoned electronic communication in favor of conventional mail for fear of NSA spying. David Jackson, *Carter uses snail mail to evade NSA*, USA Today, Mar. 24, 2014. A recent poll indicated that nearly half of American adults were changing their online behavior in response to NSA surveillance programs. Julian Hattem, *Many say NSA news changed their behavior*, The Hill, Apr. 2, 2014.[12]

---

[11] Such concerns have generated an industry purporting to preserve privacy in electronic communications. Victor Li, *Tools for lawyers worried that NSA is eavesdropping on their confidential conversations*, ABA Journal, Mar. 30, 2014 ("[L]awyers should assume all of their conversations are subject to NSA surveillance and take steps to protect confidential information").

[12] Available at http://thehill.com/blogs/hillicon-valley/technology/202434-poll-nearly-half-say-nsa-news-affected-behaior.

As Justice Sotomayor expressed in the more limited context of geo-positional monitoring, the warrantless accessing of the contents of Americans' electronic communications chills associational and expressive freedom in a manner that may alter the relationship between citizen and government in a way inimical to democratic society. *Jones v. United States*, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring). The vagueness and breadth of § 702, as to the surveillance of Americans, renders the statute invalid because of the resulting chill Americans experience in their exercise of protected speech and association.

C. Without Regard To The Constitutionality Of The Program, If The Acquisition, Retention, Accessing, Dissemination, And Use Of Electronic Communications Exceeded The Authorizations, These Intrusions Are Unlawful For That Reason Alone And Require Suppression Of The Derived Evidence.

Even if the statute were constitutional, collection of electronic communications and the execution of the acquisition, retention, and accessing procedures must be within the scope of the authorizations. Without discovery regarding the particular actions that led to the searches and seizures in the present case, the Court must obtain extensive background material in order to assure the government's surveillance activity was lawfully "conducted" within the meaning of 50 U.S.C. § 1806(g). We know from the cases declassified from the FISC that there has been extensive electronic surveillance that went beyond the authorizations. *See*, *e.g.*, *[Case Name Redacted]*, 2011 WL 10945618 at *2-6 (FISC required further briefing by the government because "it appeared to the Court that the acquisitions described in [a recent government letter to the Court] exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part,

fall outside the scope of Section 702"); *see also* CR 489 at 19 (quoting four other declassified FISC opinions discussing the government's compliance failures).

D. The Collection Of Telephone Metadata Under Section 215 Of The Patriot Act, As Well As Other Warrantless Surveillance, Violated The Fourth Amendment And The Underlying Statutes, Thereby Requiring Suppression Of The Fruits Of The Surveillance.

In addition to the FAA surveillance that is the subject of the government's post-trial notice, numerous other methods of surveillance and information-gathering programs have come to light since the trial in this case. The defense highlighted some of these programs and requested – but was denied – discovery with respect to any such surveillance. CR 489 at 20-25. Some programs, like the Patriot Act's § 215 bulk telephony collection program, have been publicly acknowledged by the government and have been the subject of litigation. Other programs have not. What is clear, however, is that the government does not believe it is obligated to provide notice to criminal defendants of these activities.[13] The defense has not been informed of any additional surveillance activities either through formal notice or the discovery process, despite its continued belief that such government activity likely occurred and requires redress. In this vacuum, the defense has no alternative but to move for suppression of all fruits of undisclosed surveillance, including tactical investigatory decisions made after the alleged unlawful surveillance. *See Murray*, 487 U.S. at 542.

---

[13] Where this type of material, or the fact of the underlying surveillance itself, implicates *Brady* or is otherwise discoverable, the government presumably would at least be required to present it to a court pursuant to the Classified Information Procedures Act (CIPA). The defense obviously does not know if that occurred in this case. To the extent it did, the defense requests that the Court revisit any pretrial CIPA rulings in light of the testimony presented at trial to assess whether the material would have been favorable to the defense and whether it called into question the government's narrative of the investigation. *See* Second Motion For A New Trial.

Because § 215 is one of the few publically acknowledged surveillance program, and because of the strong possibility that the defendant's telephone metadata was collected, the Court should address the lawfulness of the program and conclude, as did the Privacy and Civil Liberties Oversight Board, that the program violated the underlying statute and likely the First and Fourth Amendments.[14]

The telephony metadata program, operated pursuant to § 215 of the Patriot Act (codified in FISA as 50 U.S.C. § 1861), is an indiscriminate, bulk collection program whereby the government requires telecommunications companies to provide to it – apparently on an on-going, daily basis – all telephone metadata for all calls made by all people using that telecom service. *See Klayman v. Obama*, 957 F. Supp. 2d 1, 14-19 (D.D.C. 2013) (providing an extensive description of the program). The government then retains those extensive call record details for five years. The goal of these mass seizures is to create a database of call records that can later be queried when a phone number of interest is discovered. The program allows for government analysts, with no judicial oversight whatsoever, to query the bulk § 215 database for up to three steps – or "hops" – from the target phone number. In other words, the government will search for all calls made from a target phone to any other phone (first "hop"), then for any calls made by that second phone to other phones (second "hop"), and then again from any of those phones in the second hop to any others (third "hop"). As noted in *Klayman*, the sheer quantity of phone numbers accessed through a single query can be staggeringly large. *Id.* at 16-17 (noting that if each phone number hypothetically called 100

[14] Given the scope of the § 215 program, the Court should assume its capture of the defendant's telephone metadata unless the government affirmatively represents to the Court that no such information was collected.

different numbers over the course of a five year period, a single query extended to the third "hop" would generate 1,000,000 total hits).

Not only has the revelation of mass, indiscriminate collection of American citizen's phone records generated significant public backlash, it has also been met with skepticism by those analyzing it from a legal standpoint. For example, the Privacy and Civil Liberties Oversight Board was charged with assessing § 215 and ultimately determined that the program was unlawful on statutory and likely constitutional grounds. The PCLOB report noted that while the underlying statute was "designed to enable the FBI to acquire records that a business has in its possession, as part of an FBI investigation, when those records are relevant to the investigation," the "operation of the NSA's bulk telephone records program bears almost no resemblance" to that textual authority. PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 10 (Jan. 23, 2014).

Specifically, the bulk collection exceeded the statute in four primary ways. First, the statute requires a connection to a specific FBI investigation at the time of collection, which is not the case under this mass acquisition program. Second, the statute requires that the records collected be "relevant" to an FBI investigation, which, again, is not the case under this program unless the word "relevant" is redefined "in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records." *Id*. Third, the NSA program requires the telecom companies to furnish call records on a daily basis as they are generated, as opposed to simply turning over records already in their possession, "an approach lacking

foundation in the statute and one that is inconsistent with FISA as a whole." *Id*. Finally, the statute only permits the FBI to collect records – "it does not authorize the NSA to collect anything." *Id.*

The PCLOB also concluded that the § 215 mass telephony collection program violates the Electronic Communications Privacy Act and raises concerns under the First and Fourth Amendments to the Constitution. Similarly, in *Klayman*, the district court granted a preliminary injunction in a civil case challenging § 215 collections because of the high likelihood that the plaintiffs would succeed on their Fourth Amendment argument. 957 F. Supp. 2d at 9-10. In rejecting the government's attempt to evade Fourth Amendment analysis by shoe-horning the § 215 program into the pen register/trap and trace reasoning of the Supreme Court in *Smith v. Maryland*, 442 U.S. 735 (1979), *Klayman* recognized that the information learned, and the privacy intrusions at issue, are far more extensive under § 215:

> The question before me is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, "whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment" – under the circumstances addressed and contemplated in that case – is a far cry from the issue in this case. Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances – the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies – become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.

Id. at 31 (emphasis in original; internal citation omitted); *but see ACLU v. Clapper*, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2014) (holding that *Smith* was the relevant precedent in analyzing § 215 and finding the surveillance program constitutional).

Based on the public outcry and the various legal analyses and arguments, President Obama has initiated and proposed changes to the § 215 program such as limiting the number of "hops" to two and requiring the telecom companies to maintain the call record data rather than having the NSA collect and retain it. White House press Release, *Fact Sheet: Review Of U.S. Signals Intelligence*, Jan. 17, 2014. While this likely reflects the growing belief that § 215 is constitutionally (and statutorily) suspect, it does not change the issue in this case because any use of that program necessarily predates these recent efforts at reform. There are many nuanced and complex legal and factual questions that should be briefed in full by informed counsel if the government gathered metadata regarding Mohamed's telephone or internet communications.[15] With adequate discovery, the defense will elaborate on the legal significance of the specific application of the program to the facts of this case.

E. The Court Should Grant An Evidentiary Hearing To Allow The Defense To Controvert Applications For FISA Warrants In This Case Under The Supreme Court's *Franks v. Delaware* Decision.

The defense has requested a *Franks* hearing to challenge alleged deficiencies in the government's applications for FISA surveillance, both in terms of material misstatements and material omissions. *See* CR 55 at 17, 489 at 41-42 (citing *Franks v. Delaware*, 438 U.S. 154 (1978); *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985)). In response, the government invoked

[15] In addition to telephone metadata, the government apparently operated an internet metadata program until 2011 that was even more extensive then the telephone program and may well have captured communication data regarding the defendant. Glenn Greenwald & Spencer Ackerman, *NSA collected US email records in bulk for more than two years under Obama*, The Guardian, June 27, 2013.

FISA as a shield to prevent disclosure of the application materials, and the *Franks* standard of "a substantial preliminary showing" as a sword to argue that the defense has failed to meet the threshold standard to be entitled to a hearing. *See* CR 88 at 33-37. Under the Fourth Amendment norm, the defendant in *Franks* has access to the underlying warrant applications, so placing the burden of a "substantial" showing on the defense provides a logical balance between upholding a defendant's rights to test the government's ex parte representations to the judge issuing the warrant and preventing frivolous claims and unnecessary hearings. Here, however, in the context of affidavits withheld from the defense, allowing the government to hide behind the *Franks* burden of production, while withholding the very material traditionally necessary to meet that standard, would render illusory the *Franks* protection of the judicial role in issuing warrants. In any event, the material omission from any FISA application that § 702 surveillance was previously used, and the revelations that the relevant national security agencies have lacked candor in dealing with the judiciary, provide sufficient preliminary bases for a *Franks* hearing.

The defense seeks a *Franks* hearing to challenge the validity of representations made to the FISC. Those representations led that court to find probable cause, a determination the defense continues to believe was erroneous. The existence of previously undisclosed surveillance – both in terms of the § 702 surveillance at issue here as well as the wealth of public leaks regarding massive U.S. spying on communications generally – raises serious questions about whether the government "manipulate[d] the inferences" drawn by "reporting less than the total story" to the FISC. *Stanert*, 762 F.2d at 781. Given the FISA prohibition on use of First Amendment activities, 50 U.S.C. § 1805(a)(2)(A), the defense should be in the position to argue to the Court that, based on all the

facts now known, the "total story" was not provided to the FISC, rendering the FISA warrant invalid. Furthermore, because this Court reviewed the FISA applications before trial, but was not informed of the prior warrantless surveillance until after trial, the FISA applications materially omitted an explanation of prior surveillance and possibly the genesis of evidence relied upon. Either circumstance should suffice to entitle the defense to an evidentiary hearing.

Additionally, the government's recent conduct in terms of candor to the court in federal cases involving national security issues casts serious doubt on any presumption of regularity that might otherwise attach to the government's ex parte representations. In one case, the government "provided false and misleading information" to the court regarding the existence of certain documents, then asserted the "untenable" position that misleading the court was permissible "to avoid compromising national security." *Islamic Shura Council of S. Cal. v. FBI*, 779 F. Supp. 2d 1114, 1117 (C.D. Cal. 2011). In another case, which involved a challenge to a plaintiff's placement on the No-Fly list, the government invoked national security, attempted to dismiss the action based on the state secrets privilege, and insisted on numerous ex parte proceedings before finally acknowledging – after years of litigation – that the plaintiff was not a threat to national security and that her placement on the No-Fly list was due to an FBI agent's clerical error. *See* Attachment to Notice Regarding Redacted Order, *Ibrahim v. Dep't of Homeland Sec.*, No. 3:06-cv-0545 (N.D. Cal. Feb. 7, 2014), ECF 703-1; David Kravets, *How Obama Officials Cried 'Terrorism' to Cover Up a Paperwork Error*, Wired, Feb. 11, 2014.

In a case like the present one, litigating recently disclosed surveillance activity, the district court chided a government position – based on undisclosed facts known only to the government –

by noting that "[c]andor of this type defies common sense and does not exactly inspire confidence!" *Klayman v. Obama*, 957 F. Supp. 2d 1, 27 (D.D.C. 2013). Even when appearing before the FISC, the government has "made misrepresentations and inaccurate statements" and engaged in "systematic noncompliance" with certain procedures required by that court. *Id*. at 18. With respect to surveillance pursuant to § 702, the FISC noted similar concerns, and in 2011 "found that the Government had misrepresented the scope of its targeting of certain internet communications." *Id*. at 19. To prevent such occurrences here, adversarial testing at an evidentiary hearing is required.

The defense has highlighted numerous reasons why the Court should be wary of the government's ex parte representations, both based on the facts of this case and the government's actions in other cases where national security is invoked to prevent defense access to otherwise discoverable material. Given the cloak of secrecy the government has cast over material necessary to raise an ordinary *Franks* challenge, this Court should find that the defense has made a sufficient showing to warrant a hearing in the event the Court does not otherwise rule in the defendant's favor with respect to dismissing the indictment or suppressing all FISA-derived evidence.

III. The Defense Requests That The Court Reconsider Its Discovery Ruling In Light Of The Filing Of The Motion To Suppress.

In its denial of the defense post-trial discovery motion, the Court indicated that the motion may be reconsidered upon filing of the motion to suppress and receipt of ex parte documents from the government. CR 499 at 8. The defense requests that the initial motion be reconsidered and that, in addition to the questions provided in the discovery motion, CR 489 at 56-58, the Court consider the following:

Generally, with respect to the extent, source and use of the information at issue:

- What evidence or information was gathered through surveillance about Mohamed;
- When was such evidence or information gathered;
- Under what programs and authorizations was such evidence or information gathered;
- How was such information accessed and used;
- Which agency initially obtained the information through the FAA;
- Who or what was the initial selector or target;
- Which agency maintained the database into which the initial information was placed;
- Was the information obtained through Prism or Upstream or other program;
- Was the information obtained from a "packet" that contained other person's emails, phone calls, or other material;
- Who, from which agency, conducted what investigations or inquiries of any sort about the initial information about Mohamed or any identifying information (inquiry needs to be made about all such inquiry, investigation, search, in whatever form and by whatever name and the results of all such activity);
- Were any private contractors involved in the acquisition, review, use, dissemination, retention, of any of the information about Mohamed or utilized in this case;
- When information about Mohamed was first obtained or noticed and who, from which agency, determined what about him (specifically was he believed to be a United States person? If so, why? Based on what information or inquiry or search? If not, why not? What efforts were made to determine whether Mohamed or the identifying information or email address or phone number or ISP, or other identifier, was related to a United States person);

- Who, from which agency, had access to or knowledge of whatever information was initially obtained that related to Mohamed and in what ways was that information disseminated, to whom, and with whom was it discussed;

- What persons in what agency were aware of the FAA-obtained information when a decision was made to seek a FISA warrant or start some sort of investigation of or surveillance, whether through FISA, or otherwise, against or about Mohamed;

- Were there any interagency transfers or any of the information at issue in this case (if so, why, by whom, on what basis, under what protocol, and for what purpose);

- What persons from what agencies prepared the FISC affidavit that related to Mohamed;

- What information obtained or derived from § 702 activity was provided to the FISC in any such affidavit;

- Were any queries of any data bases containing § 702 information made using any information related to Mohamed (if so ,what, by whom, which data base, and how was any search information utilized) (if no such queries were made, what process was utilized to learn about the Mohamed related information);

- What if any information from any § 702 database was provided to any FBI or U.S. attorney personnel in Oregon (if yes, when, by whom, to whom and how was what information identified as relevant to an investigation);

- What queries were made of what databases and by whom and from what agency utilizing the information obtained through the FAA activity that related to Mohamed;

- What information was obtained as a result of any such queries;

- Was any such information included in any form, directly or indirectly, in any application made to the FISC related to Mohamed;

- Was any such information known to any persons who participated in any decision-making processes regarding any investigative, surveillance, or other activity related to Mohamed;

- Was there ever any discussion about purging the information that related to Mohamed that was obtained through FAA activity;

- What minimization and targeting procedures and interpretive instructions were in effect at the time any such evidence or information was gathered, and how were those procedures implemented (i.e., who was being targeted, what was the basis for that targeting, and what minimization procedures were used during that targeting) (the written procedures should be produced so additional questions can be propounded);

- Which agencies' minimization procedures were at issue in this investigation;

- How, when, and to or by whom was such evidence or information disseminated, accessed, or otherwise used;

- What dissemination procedures and interpretive instructions were in effect at the time any such evidence or information was gathered, accessed, and disseminated or otherwise used, and how were those procedures implemented relative to evidence or information gathered related to Mohamed;

- What justification was relied upon in conducting § 702 surveillance, including but not limited to any FISC decisions relative to such surveillance;

- What, if anything, was this Court told about § 702 surveillance relative to Mohamed (or other persons relevant to this case) in deciding pretrial discovery and suppression motions and trial evidentiary rulings;

- What, if anything, was the FISC told about § 1881a surveillance relative to Mohamed (or other persons relevant to this case) in approving any FISA warrants in this case.

With respect to other surveillance, given the public accounts of the extent of surveillance, the following questions should be asked.

- What evidence or information was gathered pursuant to other sections of FISA, including but not limited to 50 U.S.C. §§ 1842, 1861, 1881b, and 1881c;

- What evidence or information was gathered pursuant to other surveillance or information gathering programs implemented by any government agency that

has not been disclosed to the defense, including but not limited to the use of malware or spyware to access and exploit Mohamed's computer, and any other surveillance activities conducted by any government agency;

- How was any such evidence or information identified, collected, and retained;

- How, when, and to or by whom, was any such evidence or information disseminated, accessed, or otherwise used;

- What was the legal justification, if any, related to the collection and use of such evidence or information;

- What were any minimization, targeting, retention, and dissemination procedures and interpretive instructions in place relative to any surveillance described above and how were those procedures implemented relative to Mohamed;

- What, if anything, was this Court told about such evidence or information (and the means by which it was obtained) in deciding pretrial discovery and suppression motions and trial evidentiary rulings;

- What, if anything, was the FISC told about such evidence or information (and the means by which it was obtained) in approving any FISA warrants in this case.

A full constitutional analysis of the implications of warrantless surveillance cannot be conducted without answers to these questions, which seek accurate information about the acquisition, filtering, storing, querying, and use of Americans' communications. The traditional adversary system provides the appropriate forum to obtain these answers.

Conclusion

In place of the robust protections for Americans' privacy in their communications under the First and Fourth Amendments, § 702 provides only flaccid and illusory imitations of those protections, leaving Americans open to general searches of their emails and telephone calls and

chilled in their private communications. This Court should defend the Founders' approach to limiting governmental intrusions on privacy, whether under the Constitution or through construing the statute to require coextensive protections, by suppressing the products of the warrantless surveillance in this case. For all the reasons set out in the foregoing memorandum, the Court should vacate the conviction, grant a new trial, and suppress all evidence and other derivative uses of the unlawful surveillance, including the fruits of any action taken or decisions based on the unlawful surveillance activity.

Dated this 4th day of April, 2014.

/s/ Stephen R. Sady
Stephen R. Sady
Chief Deputy Federal Public Defender

/s/ Steven T. Wax
Steven T. Wax
Federal Public Defender

/s/ Lisa Hay
Lisa Hay
Assistant Federal Public Defender

Mark Ahlemeyer
Research & Writing Attorney